UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/705,396	11/12/2003	Nadarajah Asokan	39700-583001US/NC37029US	4400

64046 7590 02/12/2010

MINTZ, LEVIN, COHN, FERRIS, GLOVSKY AND POPEO, P.C
ONE FINANCIAL CENTER
BOSTON, MA 02111

EXAMINER	
D AGOSTA, STEPHEN M	

ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
02/12/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/705,396	ASOKAN ET AL.	
	Examiner	Art Unit	
	Stephen M. D'Agosta	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 January 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2,3,7-9,13,15,17,24-26 and 32-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *7-9, 13, 15, 17, 24, 26, 32 and 34-40* is/are allowed.

6)☒ Claim(s) *3,25 and 33* is/are rejected.

7)☒ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.

1. Claims 2, 24, 26, 32 and 34-36 are allowed.
2. Broader claims 3, 25 and 33 are still rejected (see below).

> Regarding claims 3 and 33: There were previously no dependent claims that were objected to as being novel which depended directly from claims 3 or 33. Since these claims were more broadly written than the other allowed claims, they stand rejected as well.

> In the examiner's opinion, newly amended claim 25 does not include the exact wording that the previous claims 25 and 27 recited, hence it stands rejected as well.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 25 and 33 rejected under 35 U.S.C. 103(a) as being unpatentable over RFC 2977 and further in view of Tsuda and Lee and Leung.

As per **claims 3, 25 and 33**, RFC 2977 teaches a method comprising:

receiving a message from subscriber's user equipment, said message indicating that an address of a certificate provisioning gateway for certificate issuance and delivery procedure in a visited network is requested by the subscriber's user equipment (Section 3 teaches a "Basic Model" whereby a roaming user connects to an "agent/gateway

function" which then seeks to perform back-end operations to determine if the local or home domain must be contacted to verify the user. See figure 1.),

Obtaining, in response to receiving the a/the message, subscriber's location information maintaining in a mobile communication system subscriber's location/network information (RFC 2977 teaches the concept of Mobile IP where a user roams as well as home and foreign/local domains which inherently ***requires the "network" to keep track of where the mobile unit is located***. Furthermore, the HLR and VLR components perform this same task. Also Mobile IP tracks/understands the network-address of which LAN segment the user is connected to.);

the certificate provisioning gateway serving at least one certificate authority, the message further containing the address of the certificate provisioning gateway and authenticating the subscriber AND transmitting after the authentication via a channel to the subscriber's user equipment at least part of information required for a certificate issuance (figures 1-2 show and Sections 4-5 teach requests/serving of home/foreign authority. Furthermore, Mobile IP inherently requires interaction between the home and foreign authorities to verify/authenticate a user and IP routing inherently requires the use of a node's exact address in order for a message to be sent to it);

determining, on the basis of the subscriber's network information, an address of the certificate provisioning gateway (figures 1-2 and sections 4-5 discuss the interaction between home/local authorities when a Mobile IP user roams from one domain to another domain):

checking whether or not the address in the message is the same as the address of the certificate provisioning gateway determined on the basis of the network information (figures 1-2 and sections 4-5 teach that the network/IP address of the Mobile IP user will be identified and a decision made as to contact the home domain to verify/authenticate the user); and

but is silent on use of location information AND if they are **not** the same, using the address determined on the basis of the location information AND transmitting to the subscriber's user equipment at least part of information required to obtain a certificate from the certificate provisioning gateway having the address of the certificate

provisioning gateway AND transmitting via an authenticated channel for service in another network than a home network of the subscriber, said at least part of the information comprising information required to obtain a certificate from the certificate issuance service in the other network.

RFC 2977 focuses more on the underpinnings of IP and MOBILE IP where the user's IP address and current Network Address are used to determine the "location" of the user and if assistance from the Home (authority/agent) is needed. The term location for RFC 2977 is not a geographic position, but rather a correlation between the user's home IP address and their current connection to a LAN segment (eg. they are in their home domain/location if the network LAN Addresses match and/or they are in a foreign domain/location if they do not match). RFC 2977 teaches the concept of LOCAL and HOME AAA functions (see figure 1 where HOME is the user's home network and LOCAL can be a foreign/visited network based on the user's current location. The concepts put forth in "The basic model" (page 5 to 6) is that the Local AAA will check with the Home AAA as required. Hence if the user needs information and attempts to contact its Home AAA, the Local network will check/compare the address of the AAA function it is attempting to contact, hence the Local AAA will be used instead of the Home AAA. RFC 2977 also puts forth a connection between the Local and Home AAA's (see figure 2) and that data can flow between them for authentication purposes. Therefore, one skilled would use the "most local" authority/AAA server when roaming since it would be time-consuming to contact the Home Authority/AAA especially since RFC 2977 teaches that the Home and Local AAA's provide cross-authentication to verify each user when they roam into foreign networks.

As previously put forth in earlier rejections, **Tsuda** teaches a network using Mobile IP and AAA protocols for general authentication and Accounting (eg. for a certificate issuance service in another network than a home network. See figure 10 shows mobile user registering with a foreign agent in a non-home network. Abstract and figure 1 show a system that allows a user to be authenticated to roam to various networks and use services whereby AAA information is transmitted to/from a user's

device. Also see figure 6, Step 2 and figure 10 which shows an authentication procedure and figure 10 shows overall procedure whereby data is sent to/from the mobile's AAA-H/AAA-V servers in order to authenticate said user as he roams. Figures 10-11 show mobile authenticating with AAA and P#186 discusses use of certificate issuance via certificate authority. Furthermore, he also teaches a Mobile IP network, figure 1 shows a mobile user who has roamed from a home network #1001/#1010 to a visited network #1002/#1010 connected via IP which inherently subnets a network into smaller networks and their location is known based on where the engineer has positioned the local access router/BTS. Lastly, the mobile network maintains user location in an HLR and Tsuda teaches both home and foreign networks, P#67 and P#71, which inherently describes the concept of *knowing where the user is (eg. maintaining a subscriber's location in the network)* since it is either in the (one) home network or in any of other foreign networks -- see figure 18 which shows multiple foreign subnets, #1002/#1004. Tsuda clearly shows multiple networks connected each having an AAA/Certificate server (figures 1-2). Hence a de-centralized AAA server design would inherently require the user's authentication request to be handled by the "local" AAA server. Figure 3 shows a connection from AAA #70 to AAA #60 on different networks with a "broker" in between (reads on a CA Provisioning Gateway). Also see figure 6 which shows that the two networks/AAA's interact, steps 101-109.

With regard to using geographical position data to assist with network configuration/authentication, **Lee** teaches an "automated process" to enable nomadic roaming such that a user can request connectivity to a device whereby an agent determines the user has roamed into a visited network and translates the request into a connection to a new, similar device AND The IP address of the ***user's current location is used in concert with the terminal's identifier,*** which is itself an IP address, to route incoming computing communications connection requests to the current location of the user. (Abstract). This alleviates the need for the user to track/determine if they have roamed into a visited network and then request a new device address. Furthermore, Lee puts forth multiple connected networks that use various services from the different networks. One skilled understands that a network design would either be centralized or

distributed. Thusly, the AAA/Certificate servers would either all be at one location or spread out across the network -- forcing the user to either always contact the central server or contact a local server. Figure 4 clearly shows that the user uses both voice and data services and that the network tracks the user across multiple networks (See Care-of-Address and various TID's). Therefore the use of one or multiple "certificate authorities" is viewed as a **design choice**.

Regarding sending information so that a roaming user can authenticate (eg. via AAA/Certificate authority as taught by RFC/Tsuda/Lee) in another network (eg. foreign/visited network), the examiner puts forth **Leung** who teaches data flow from the Home network to the Visited network (figures 1-3) in order to fully authenticate the user in said Visited network (eg. the data flow supplies necessary information to obtain registration. Of significant importance is the fact that Leung teaches contacting the Home network for verification which can be broadly viewed as contacting an "authorization agent/function" which reads on an AAA/Certificate server: (see C1-C2)

Now, suppose that Mobile Node 6 is removed from its home base network segment 12 and roams to a remote network segment 14. Network segment 14 may include various other nodes such as a PC 16. The nodes on network segment 14 communicate with the internet through a router which doubles as Foreign Agent 10. Mobile Node 6 may identify Foreign Agent 10 through various solicitations and advertisements which form part of the Mobile IP protocol. When Mobile Node 6 engages with network segment 14, Foreign Agent 10 relays a registration request to Home Agent 8 (as indicated by the dotted line "Registration"). The Home and Foreign Agents may then negotiate the conditions of the Mobile Node's attachment to Foreign Agent 10. For example, the attachment may be limited to a period of time, such as two hours. When the negotiation is successfully completed, Home Agent 8 updates an internal "mobility binding table" which specifies the care-of address (e.g., a collocated care-of address or the Foreign Agent's IP address) in association with the identity of Mobile Node 6. Further, the Foreign Agent 10

updates an internal "visitor table" which specifies the Mobile Node address, Home Agent address, etc. In effect, the Mobile Node's home base IP address (associated with segment 12) has been shifted to the Foreign Agent's IP address (associated with segment 14).

It would have been obvious to one skilled in the art at the time of the invention to modify RFC 2977, such that it uses location information AND if they/CA's are not the same, using the address determined on the basis of the location information AND transmitting to the subscriber's user equipment at least part of information required to obtain a certificate from the certificate provisioning gateway having the address of the certificate provisioning gateway, to provide means for the mobile device to quickly ascertain AAA information/authentication by using a local AAA/CA server if/when roaming in a foreign network.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Stephen M. D'Agosta whose telephone number is 571-272-7862. The examiner can normally be reached on M-F, 8am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lun Yi Lao can be reached on 571-272-7671. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Stephen M. D'Agosta/
Primary Examiner, Art Unit 2617